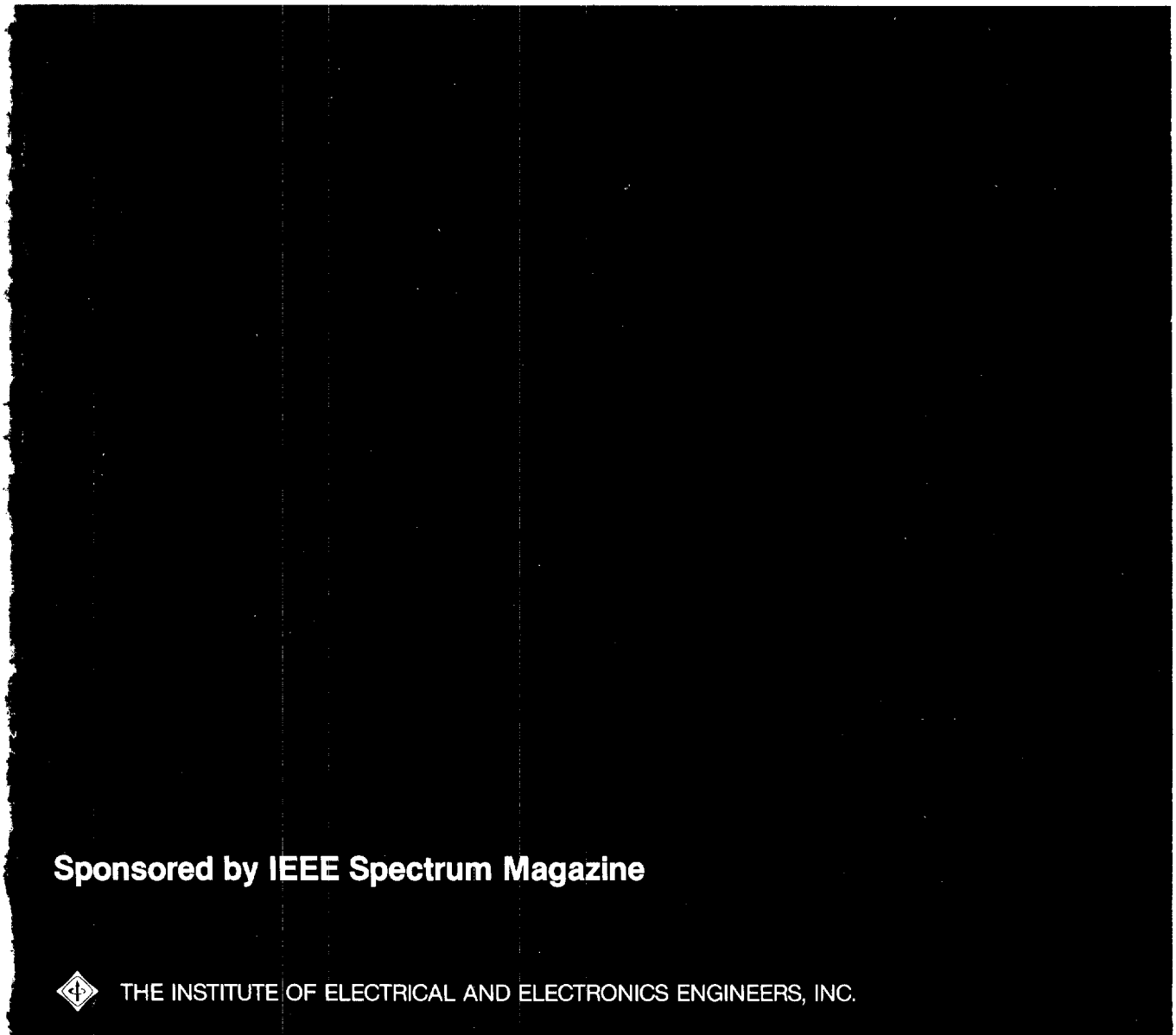
A round-table report

MANAGING THE FLOW OF TECHNICAL INFORMATION
AN INDUSTRY/GOVERNMENT DIALOGUE

June 2, 1982



Sponsored by IEEE Spectrum Magazine

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

MANAGING THE FLOW OF TECHNICAL INFORMATION
AN INDUSTRY/GOVERNMENT DIALOGUE

Sponsored by *IEEE SPECTRUM* Magazine
with the participation of
GEORGE A. KEYWORTH
SCIENCE ADVISOR TO THE PRESIDENT

June 2, 1982

Washington, D.C.

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600180007-9

Copies of this report may be ordered from Single Copy Sales Department, IEEE Service Center, 445 Hoes Lane, Piscataway, N.J. 08854. Telephone: (201) 981-0060.

Member price: $7.50
Nonmember price: $15.00

Approved For Release 2005/11/28 : CIA-RDP91-00901R000600180007-9

Contents

Meeting participants

From Industry

Henry Bachman, vice president, Hazeltine Corp.
Erich Bloch, vice president, IBM Corp.
Edward David, president, Exxon Research and Engineering
Grant Dove, senior vice president, Texas Instruments Inc.
John Ellicott, partner, Covington & Burling
Fred Garry, vice president, General Electric Co.
William Howard, vice president, Motorola Inc.
Gordon Moore, chairman, Intel Corp.
Robert Schmidt, vice chairman, Control Data Corp.
M.P. Wilson, associate executive director, corporate analysis division, Bell Laboratories.

Observers

Rosemary Chalk, American Association for the Advancement of Science
John C. Crowley, Association of American Universities
Leo Fanning, IEEE Washington Office
Ruth Greenstein, National Science Foundation
Richard Meserve, National Academy of Sciences
Harold Relyea, Congressional Research Service
Mitchell Wallerstein, National Academy of Sciences

From Government

George A. Keyworth, presidential science advisor
Stephen Bryen, deputy assistant secretary of defense for international trade and security policy
Bohdan Denysyk, deputy under secretary of commerce for export administration
Steven Garfinkle, director, Information Security Oversight Office, General Services Administration
Jan Herring, chief, Technology Transfer Assessment Center, Central Intelligence Agency
Ernest Johnston, senior deputy assistant director, economic and business affairs, State Department
Donald Langenberg, deputy director, National Science Foundation
Michael Lorenzo, deputy under secretary of defense for defense research and engineering
Edward McGaffigan, assistant director for international affairs, Office of Science and Technology Policy
John McMahon, deputy director, Central Intelligence Agency
Joseph Smaldone, chief, arms licensing division, Office of Munitions Control, State Department
Gus Weiss, staff member, National Security Council

Meeting chairman

Ellis Rubinstein, senior editor, news operations, *IEEE Spectrum*

Meeting secretary

Paul Wallich, associate editor, *IEEE Spectrum*

Introduction

The easiest way to keep high technology from being stolen by competitors or adversary nations is to build impenetrable walls around every high-technology project. But those walls may also stop the kind of cross-fertilization of ideas between researchers, often in diverse fields, that makes innovation possible.

The United States has confronted the delicate balance between scientific freedom and national security since World War II, when developments on the forefront of physics were used to gain victory on the front line of battle. Although security was strict during the war, the Government loosened restrictions on the free flow of information in most areas during the 1950s and 1960s, in the explicit recognition that there was more to gain from unfettered research than there was to lose from technology theft.

In the 1970s, this attitude began to change; in order to keep both militarily critical products and the basis of its high technology from leaking to countries such as the Soviet Union, the United States began placing restrictions on foreign access to research done within its borders. J. Fred Bucy, president of Texas Instruments, chaired a Defense Science Board task force that issued a report in 1976 outlining how the United States might better safeguard its militarily critical technology. That report recommended a revamping of the export control structures in place then and now, so that controls would focus on the knowledge and critical equipment required to make sophisticated end products, rather than on the export of the products themselves. The reaction of companies affected by export controls was mixed; some anticipated the easing of product restrictions, while others felt that controls on technical information would simply add one more layer to an already burdensome thicket of regulations. For the most part, however, companies remained silent and complied with the regulations as well as they could understand them.

In 1980 and 1981, possible restrictions on publication of research in cryptography brought many members of the academic community out in full force against perceived Government censorship. The debate was crystallized by a session on January 7, 1982 at the annual meeting of the American Association for the Advancement of Science. In that session, which was titled "Striking a Balance: Scientific Freedom and National Security," Admiral Bobby Ray Inman, then deputy director of the Central Intelligence Agency, said that voluntary prepublication review should be considered for any information that could aid "potential adversaries" and extended the definition of adversary to include economic as well as military competitors.

Committees were set up at the National Academy of Sciences and elsewhere to deal with the problem of information controls as they affect the academic community, but industry remained silent for the most part.

In the course of preparing an article on industry views of information-control policy, *Spectrum* held discussions with Presidential Science Advisor George A. Keyworth on the possibility of a round-table discussion to bring together industry and Government leaders for an airing of views. Those who participated in the meeting did so with an understanding that their remarks would not be attributed without consent and that Dr. Keyworth could excise certain portions of the record if national security considerations merited. With few exceptions, none took advantage of that opportunity, and no excisions were made (Unattributed remarks will be found in the appendix.)

What follows is an annotated transcript of *Spectrum*'s June 2 round table, edited to omit certain portions of the discussion not germane to information-control policy.

—*Paul Wallich*

Executive summary

Participants agreed that the current system of export controls on information does not work as it ought to. Industry participants complained that paperwork involved with regulations hampers trade and questioned whether they actually limited the spread of militarily significant information, while government representatives cited insufficient staff as a problem in handling licensing, and also noted that covert operations by Soviet-bloc nations could render laws controlling export of technical information irrelevant. Among specific concerns were that:

- Regulations are so complex and confusing that many do not understand their intent. Some companies may seek unnecessary licenses out of uncertainty.
- Activities in support of the U.S. position as second leading arms dealer to the world may already have compromised much militarily significant technical data.
- Regulations on exports do not directly address the problems of espionage and theft.
- As long as other nations possess the same high technology, limiting export of technical data or products by U.S. companies acts only to hurt the U.S. economy, without protecting information.
- Regulations on technical data flow may hamper the operations of multinational companies, which "export" information even though it never leaves corporate channels.
- A lack of priorities for enforcing export regulations prevents the scarce enforcement resources that exist from being properly applied.

Government officials outlined a number of steps being taken to strengthen and simplify export regulations, including the development of the Military Critical Technologies List (MCTL) by the Defense Department. They suggested that a shift in emphasis was in progress, away from current product-related controls and toward process know-how. Among the changes they mentioned were:

- Streamlining of the Export Administration Regulations so that they could be read and understood easily.
- A periodic review of the Munitions List.
- Revision and possible dissemination of the MCTL, which currently exists only in classified form.

Industry panelists suggested, however, that simply streamlining the current set of regulations will not address the problems of espionage and that a critical technologies approach, rather than reducing regulatory problems, would simply add another layer of bureaucracy to an already complex system. They suggested a thorough overhaul of the entire export control system for information, along the following lines:

- Adopting a true list of militarily critical technologies as a basis for export controls on both products and information.
- Reviewing the list so that it remains realistic.
- Improving industrial security efforts so that companies will not be as vulnerable to espionage as they are today.
- Relying on industry's self-interest to help keep information secure, rather than imposing regulations that may hamper communication within a company as much as they retard technology transfer.

The participants agreed that a good industry-Government dialogue is needed if information controls are to serve their purpose. Some suggestions were made for the establishment of such a dialogue, but no conclusions were reached on how to do so.

Round table

George A. Keyworth, Presidential Science Advisor

Although there have been a number of these interactions between Government officials and members of the academic community, I think this is really the first broad meeting with industrial representatives. We want to establish good channels of communication between those various sectors because in many ways it is industry, not academia, that is most immediately affected by changes and policy regarding the release or report of technical information and products of course.

Certainly, we're all aiming for a position that reasonably balances the needs of the national security and the needs for scientific freedom to exchange ideas and research results. I think we have to keep our goal firmly in mind: to maintain and extend our technological edge over the Soviets. This is essential to restoring the military balance with the Soviet Union. We are unlikely to match the Soviets in quantity of either men or tanks or aircraft at any time in the foreseeable future, so we have to overmatch them in quality.

We're attempting both to slow the progress of their military establishment by denying them our critical technology and to spur American and Western innovation on militarily critical technology. The Soviet empire is our concern, not our allies with whom we share much of our most advanced defense technology: F-15s, F-16s, Sidewinders, and so on. We do want our allies to take this problem as seriously as we do because the Soviets will always find and exploit the weakest link in the chain. We're now working with the allies to try to strengthen CoCom export controls, as some of the other participants will explain.

John McMahon, Deputy Director, Central Intelligence Agency

We've been trying to scope the problem of technology transfer and what technology is being transferred to the Soviet Union, and what impact that has on the United States. A little over a year and one half ago, we conducted a study of several hundred militarily significant transfers of U.S. and Western technology to the Soviet Bloc and then asked the question: How did the Soviets get the technology and what effect did it have on their military systems? What we found was rather appalling. We were also able to determine that the mistakes that we had made in assessing missile accuracy on the Soviet missiles were not because we misjudged the evolution of Soviet technology but we did not consider the fact that the Soviets were acquiring U.S. guidance technology. We should have been looking for what that technology could do for their missile accuracy.

And so we found a rather extensive Soviet program to acquire Western technology using the KGB and the GRU. It is a very aggressive program. We found that some 75 percent of the militarily significant items of U.S. and Western technology that the Soviets had were derived from operations through their intelligence services, where they acquired information either overtly or through typical James Bond operations where they could operate against the U.S. industry and businessmen both here and abroad and against U.S. subsidiaries abroad to acquire not only plans and/or designs but even hardware. This effort spanned the entire spectrum of technology.

We also found that in addition to being able to acquire that technology which gave them capabilities in aircraft and transports, they also had the plans for the C–5A before it even flew. They had avionics, they had look-down/shoot-down radars, they had information on our Awacs radars, and when we looked at all the military industries in the Soviet Union, and we found that they had technology to aid them in the design and manufacture of their propulsion systems and their ships and their submarines, their ASW, their laser rangefinders for tanks, much of it had come from here in the United States. Then as we looked at the entire military–industrial complex of the Soviet Union to find out where they're going in the 1980s, we saw many of their plants expanding, and the Soviets do not have the wherewithal technologically to provide the manufacturing capability in those plants, so they will have to come to the West to acquire that. What we want to do is put the West on notice that the Soviets are coming after not only our advanced technology but also the simple industrial computer-driven machines, operational software, com-

p[illegible] this military complex and filling the vacant floors that now exist in these many plants. That goes to every aspect of an arsenal, whether it is tanks,

trucks, submarines, shipbuilding, aircraft, air transport. It is an awesome program and they are using their intelligence services to help them. Therefore, we view this not so much as a trade problem, but as a counterintelligence problem, and our focus with the Western nations, Europe and Japan, has been to alert those nations that they have to look at this from a counterintelligence standpoint because it is the KGB and GRU that is driving it.

Steven Garfinkle, Director, Information Security Oversight Office

There's been a great deal of publicity that the executive order signed by President Reagan on April 2 is (1) an effort to classify a great deal more information than may be classified under the existing executive order and (2) a step backwards on the issue of the classification of scientific and technological information. Both of these general statements, which have appeared often in the media, are incorrect.

The impetus for the new executive order or classification actually began before the Reagan administration. There was a consensus within the most affected executive-branch agencies that some of the so-called reforms of the executive order signed by President Carter in 1978 had resulted in administrative and litigative problems for the United States in protecting some information that clearly merited national security protection in the form of classification.

And it was to the end of cleaning up some of these administrative problems and perhaps, more importantly, these litigative problems that an effort was begun to consider amending the executive order even during the time of the Carter administration. With the onset of the Reagan administration, the most important change was that it went from an effort to amend the existing order to a new order. There are a couple of things about the new order and its effect on the information that will be under discussion today that I think are most critical.

First of all, in signing the new order the President indicated that one of the most important things about an information security system or classification system is that the information to be classified must warrant that classification. If not, if we go about classifying a great deal of information that does not warrant protection, we end up jeopardizing that information which does. Four things have to happen before we can classify information.

First, only an individual with original classification authority may classify information. Throughout the executive branch of government, worldwide, including the military, there are only about 7000 persons who have the authority to make the determination that information which has not previously been classified should be classified.

Of that 7000 approximately 1300 are authorized to classify information as "Top Secret," approximately 5000 "Secret," and the remainder "Confidential."

Second, the Government must own or control the information that is to be classified. I think that test is critical, very critical to matters under discussion today. Own or control; ownership is easy to understand, but control is not quite so easy. It's a term that scares people, but control means a lot more than just possession. The Government possesses a great deal of information that industry possesses, academia possesses. By controlling I would suggest controlling its distribution and dissemination, controlling access generally.

Thirdly, the information must fall within one of 10 classification categories. Of the four tests that I'm describing this is the least important because the categories are intentionally broad, and just about any information would fit into one or more of the categories.

And fourth, there must be a determination by the original classifier that the information if disclosed without authorization would result in damage to the national security. It has been stated over and over again that the thought process involved in this decision has been removed from the new executive order. That is contrary to our intent. There is always an inherent weighing of the factors that bear on the interest of protection and the interest of disclosure in any classification decision and any declassification decision. That will not be altered by the new order.

So what I leave you with is the idea that things really have not changed significantly from the way they are now, notwithstanding some of the articles you may have been reading which would indicate otherwise.

Joseph Smaldone, Chief, Arms-Licensing Division, Office of Munitions Control, State Department

The Office of Munitions Control in the State Department administers the International Traffic in Arms Regulations (ITAR). Our job is to regulate commercial exports of defense articles and services. Our caseload has been increasing at about a 10-percent rate compounded per year. This year we expect to process about 40 000 license applications and other requests for export approval. Translated into dollar value, last year there were about $2 billion of commercial exports of defense articles and services and about $8 billion worth of license approval.

We're not partisans, we don't get into the fracas of trying to determine whether a particular sale will or will not be made. If there are policy and security implications we refer them to the appropriate offices of Defense, State, and elsewhere and try to reconcile any differences. We make sure everyone gets to see the cases they need to see and make sure everyone gets a fair deal.

With regard to the ITAR itself, I might put to rest the rumor about a revision because I don't see any revision happening very soon. Back in December 1980, we put in the *Federal Register* a proposed revision. We got about one volume's worth of comments from the public and ever since then we've been scratching our heads wondering what to do with them. The truth is that it will take a considerable amount of time of several people getting together and reviewing that ITAR and all the comments and trying to come up with another proposed revision; as it works out we haven't had the time. We depend very heavily upon our legal counsel for this particular service and when the one person who is available to us for that purpose looks at the ITAR at the bottom of his stack, he sort of shakes his head and goes on to the next crisis. So, I don't see anything happening very soon. I would certainly like to get it out soon but I just don't see it in the cards, unless someone is willing to take us all and lock us in a closet or send us off to an island and say go to work for a month until the job is done.

Our basic problem, as I see it, is one of saturation: the caseload is getting to the point where we are on the verge of getting overwhelmed. Now, frankly, I have been there two years and I don't know what the hell people did five years ago when we only had 20 000 cases; we are now doing 40 000 somehow with the same staff. We have undertaken some new initiatives, though, which we hope will knock out this compounded rate of increase.

We've emphasized in our various briefings with industry some of the exemptions for licensing. I really feel that industry oftentimes feels the need of a security blanket and they apply for a lot more licenses than are in fact necessary, especially for technical data. And so we have been emphasizing if you have a technical data license to market things don't bother coming back and renewing it, because there is an exemption for that. If everyone does what they are supposed to do, it will cut down a couple of thousand licenses a year. At the beginning of this year, we extended the validity period of our licenses from one to two years. We hope that this also will result in a reduction of a few thousand licenses for otherwise unshipped balances of previously approved ones. Over the course of two years, we figure most exports would have taken place. It won't be necesary to renew a license to finish up shipments.

There are also efforts to remove some items from the Munitions List. These are the articles that we control. Let me say a couple of words about how things get on and off the munitions list, mostly how they get off.

We have a long-standing procedure under which a U.S. company can write to us and ask that any particular product they make which has been on the Munitions List can be removed if they make a good argument for removal. Obsolescence or widespread commercial applications, things of that nature, are among the kinds of arguments that will be entertained. So if you can make a good argument for getting something off the list, it might succeed.

The Congress is also very interested in this issue of what's on and what's off. I'm not quite sure where Congress stands because we get different winds blowing on different days. We were required last year to do a study of the Munitions List to identify what we could remove and transfer to the Commerce Department. We did the study and as a result of that we have taken

off a number of items, and one of these days the Commerce Department should get out in the *Federal Register* a notice which will effect that removal.

We are now faced under the new 1981 legislation with the continuing requirement to do a review of the Munitions List. The language of the legislation calls for a periodic review. It didn't say how often. We'll probably do it about twice a year, and we need to report to the Congress any proposed removals 30 days before we actually effect them. We just completed our first skull session on that matter and very shortly we'll be sending over to other agencies the items that we propose for their review and comment. I might add in this whole process that neither State nor Defense unilaterally has the authority to add or subtract from the Munitions List. We have to get the DOD's approval to put on or take off. Likewise, they have to come to us for any proposed change. Neither one of us can simply add to or subtract from the list.

A couple of other issues are worth including:

1. Back in 1978, we put out a piece of advice for the Defense Logistics Agency with regard to licensing requirements for foreign nationals employed by U.S. companies. The advice was one sentence which is ambiguous at best and misleading at worst. In any event, despite the fact that we wrote this letter specifically to the Defense Logistics Agency at their request, it was widely circulated throughout the Government and industry and was interpreted, because the language is not very clear, as an exemption from licensing if you've got foreign nationals working in your company on programs which involve access to technical data. It was presumed to be a licensing exemption because they were employed here in the United States.

Well, there was never any intent to do that. The regulation is clear and consistent. In order to remove that ambiguity and to confirm the requirement for a license, there will appear in our next newsletter (#94) a reiteration of the requirement to get a license if employees are foreign nationals as opposed to immigrant aliens. Those people who understand the language know there is a big difference. If foreign nationals have access to technical data, in other words, if you would have to get a license to export the data to them in their homeland, it would certainly be inconsistent to exempt them from licensing if they work in your backyard. So we confirmed the need to take care of that. We've had all kinds of screams from people: "What is this? We've got 25 000 foreign nationals working for us."

Those who are truly foreign nationals and in a situation where they are getting access to classified or unclassified technical data which would otherwise need a license ought to be regularized by means of licenses. I have not prescribed ways by which this ought to be done except to invite those industries which find themselves in this quandary to get in touch with me. I will be happy to work out some kind of mutually agreeable way of doing that.

2. The other item has to do also with foreigners and this is foreign ownership. The ITAR does not take into account foreign ownership, therefore, if one of your companies or any U.S. company is partially or even fully owned by some foreign company, we couldn't care less. We do not regulate ownership, we regulate exports. If there is going to be technical data provided to your parents or your half-brothers or -sisters, whatever the relationship might be, get the standard license. But ownership itself does not equate to export as far as we're concerned and we don't intend to regulate ownership.

One final point: we have begun a modest program to upgrade our enforcement activities. This doesn't relate so much to U.S. industry as it does to foreign industry. We're beginning to scrutinize more carefully license applications and make more end-use checks on those which appear to be questionable. We're finding much to our chagrin that not only are foreign companies oftentimes ignorant of or acting contrary to U.S. reexport provisions but certain foreign governments are in the same situation. So piecemeal and gradually as we get to it, we're bringing to their attention the fact that if they wish to continue to benefit from having access to U.S. defense articles then they need to abide by our reexport regulations.

Bohdan Denysyk, Deputy Under Secretary of Commerce for Export Administration
During the past decade, a number of forces were acting which allowed a lot of technology to go to the Soviets that should not have gone. The political climate was such that it was conducive to the removal of some items from the list that perhaps should not have been removed. In addition, the list itself was product-oriented. It focused on the export of products in the free world as well as to bloc countries and the PRC, with less emphasis on technology transfer.

How do we control technology more efficiently? The area of most concern to most people in Government is the process know-how, the recipes to make certain types of things. Fred Bucy pointed this out very, very well in his '76 report. To date we haven't done an adequate job of controlling technology. The Export Administration Act of '79 reflected movement in that direction by directing Defense to put together an MCTL focusing on identifying strategic technology for control and thus starting to deemphasize some of our product controls.

The other element of the past decade coming back to haunt us now again is the political climate. During that period even things that were on the list were not controlled. Decisions were taken that focused only on the short-term economic benefits of those sales and not the impact on long-term national security.

There is an unclassified report now available which lists with some fair detail the types of things the Soviets are after. As you know this Soviet acquisition effort is a well-organized exercise; it's not stereotyped, bumbling KGB agents who are kind of groping around. These agents are highly sophisticated, they know what they want, they know whom to approach to get it, and that's a challenging threat we need to rise to.

Currently we're trying to tighten controls on process technology. That is our primary focus. We're also trying to decontrol products which are either insignificant or which we have no resources to enforce. Embedded microprocessors in some consumer items come to mind immediately. It's getting more and more difficult to control things like that. So when we're constructing the new list those factors will be taken into account. Of course, I'm not suggesting that we will decontrol items that contain microprocessors simply because they contain microprocessors.

We are currently engaged in a two-tier approach on the regulations. The first is a general cleanup and clarification effort. That is to simplify the language to make it more readable. I've drawn the analogy of the commodity-control list to a random walk. You start at one place, they refer you to another section, and so on, and after a while you are thoroughly confused. The first exercise is to make it more readable. For example, if there is a computer entry, we will attempt to have all the relevant notes and advice and anything else you need on one or two pages that are relevant to computers so you don't have to go walking around through an inch of paper. The second part is to examine the possibility of revising the substance or size of other control systems on technical items. That'll happen about a year after we start negotiations in October with CoCom. As part of that, we will also look at ways of doing a better job in controlling technology. By a better job I don't necessarily mean broadening the controls; there are various other ways that we can look to first, such as through more private control. We could also look at ways to narrow the list of technologies to focus on items that we have substantial leads in.

Ellis Rubinstein
[Trouble with CoCom operation?]

Ernest Johnston, Senior Deputy Assistant Director, Economic and Business Affairs, State Department
The first thing to keep in mind in regards to CoCom is that although it's an organization that's existed since 1949, it exists purely on an informal basis. There is no formal commitment by any country to follow CoCom. So it is not anything that we can force our way in too much.

Without CoCom we would stand exposed completely with regard to our export controls. So it is pretty important that we have a consolidated Western position on this. Otherwise we will have technology and commodity controls which don't have much effect on the Soviet Union and which are essentially a penalty on our own exports. It is true, I think, that there are certain

things which the United States has got a monopoly on but that is not nearly so important as a control which effects the major Western industrial countries.

CoCom operates essentially three kinds of functions. One is the establishment and the periodic updating of lists of commodities that are added or subtracted in regard to the embargo that we are trying to maintain. Second, it acts as a clearinghouse for requests by member governments to ship specific items which are on the list for given reasons. And third, it coordinates the administration of enforcement activities of the countries which are involved in it.

We think that the system can work moderately well. On the other hand there is no denying the fact that the Soviet Union and the Warsaw Pact countries have obtained some equipment and technology of strategic importance from the West either through violations of controls or because some items just aren't on the list.

Since Afghanistan, we have tried with our allies to increase some of the items that we have on the Cocom lists. In mid-1980, we got tighter controls on lasers, semiconductor manufacturing equipment, and silicon material. At the same time, and this was essentially a response to Afghanistan, we went to them with a proposal for process know-how technologies which involved plants that were being constructed in the Soviet Union valued at more than $100 000 000. We went to them with a list of defense priority industries that even though there was quite a civil component in the production of these industries, we felt further restraints should be put in effect, but were not successful with that proposal. They asked that we redefine it in terms of commodities. We have begun to do this in the metallurgy area, and we think that we are very fairly close to committee agreement on several proposals.

We had a high-level meeting in January which was the first ministerial level meeting CoCom has had in the past 20 years. There was a broad agreement to work on expanding the embargo to control critical equipment and technology not covered while at the same time exempting noncritical items—agreement on improving enforcement efforts and agreement on harmonizing national licensing practices. The licensing practices of the different countries are sufficiently different that if there is not more harmony we will not be seeing the effectiveness we would like to.

We have recently submitted several proposals for embargo coverage in special areas of concern and we are completing now the submission of several scores of other proposals for consideration during the next major CoCom list review which begins in October.

We've got 12 technical subcommittees working on precisely what ought to be in those submissions, and we have depended very heavily on the work that the Defense Department has done in the militarily critical technologies area.

Last week we held a subcommittee meeting where we made some modest movement in our efforts to encourage other members to place a high priority on enforcement efforts.

We also raised the issue of problems of diversion through third countries. The United States is the only country that requires reexport licensing if a good is sent to a second country and then it's going to be transferred to a third country. Other CoCom countries rely essentially on end-use certificates.

Stephen Bryen, Deputy Assistant Secretary of Defense for International Trade and Security Policy

There are two ways to face this problem I suspect. One is to uphold property rights and do so fiercely. You see in the academic community a great deal of upheaval and ferment over what types of controls the Government may be thinking about if they are thinking about any at all, and in the business community concern about how to address the system which itself is in transition; that's one kind of perspective. The other perspective and one I can prefer—I think a lot of it has already come out today—is really that we have a management problem. We have it for two reasons: one Bo[hdan Denysyk] touched on very well is that in a sense we're all the prisoners of the past. We're trying to come to grips with that, but it creates many areas where it is difficult to work. The second reason, which John McMahon touched on and I think very effectively, is that we face organized opposition and we're not too well organized.

Then from the other speakers, from Joseph Smaldone and from Ernest Johnston, I think you had a sense that the system we have in place now is overloaded with things to do if we really would get at the problem. All of us are stretched very thin and all of us are trying to do a great deal of work which should have been done in the past.

The CoCom effort is a tremendous undertaking. It involves seeking high-level political agreement. We've got some of that for the first time in two decades. It involves then translating that down to the working level which is no simple matter even here at home.

We also have the problem that Ernest Johnston mentioned with the Third World unaligned countries, many of which are becoming increasingly technologically capable. How we handle that and our posture toward it has become a very important subject. It's an area where in the past we did virtually nothing at all. We have recently seen some very grievous examples of transfer from our own technology that has brought considerable harm to our defense efforts and obliged us to make expenditures in the hope of repairing some of these problems.

Then we have the management problem internally in each department. In Defense it's a question of interfacing system services with technical experts and developing a system that works in real time and one that is precise. It is no simple engineering problem. Anyone that's ever looked at the wiring diagram at the Pentagon quickly comes to the conclusion that it is not a good microprocessor. You also have a management problem which is the responsibility of industry, which has a common interest with Government in succeeding in this undertaking.

The responsibility of industry to, in a sense, police itself, to take action itself—that helps us carry out a common policy. That is an agreeable thing and industry is going to have to think and find committees, staff, personnel, education, all the things it's going to require to do this cooperatively with us. It's not in your interest or ours to try and have one side do it and the other side not. We really have to work this thing very much together. I know that tends to sound like a platitude but I hope it doesn't become that because the practice of working it out, making the maximum use of our different institutions is probably the most effective thing we could do within this Administration.

Michael Lorenzo, Deputy Under Secretary of Defense for Defense Research and Engineering

As you know, the MCTL was called for by the Export Administration Act of 1979. The first version was published in October 1980. We're in the second edition now for revision which will be published in October of this year. Unfortunately, it is still in classified version only.

A lot of facets of industry don't have facility clearance. They're really in the dark so to speak. For example, our instrumentation industry is dependent on exports for livelihood and they do need guidance. However, we're using industry groups to give them that guidance. For example, we're using the Mapag [Multi-Association Policy Advisory Group] to review the list.

It gets good technical input, it gets the practical bottom line input. I just came from the industrial sector, and you do have to make a profit and be practical as well as being bureaucratic in trying to control everything.

There is a bottom line and that's to make a profit and pay people.

First of all, a little bit of levity, I ran across Bill Perry recently, a former OUSDRE, and he said, "Gee, I hear all about the technology transfer leaks; to me that is good news. We must still have a technological lead over the Soviets since they're still trying to steal our Western technology." So that is one way of looking at it.

[Outlines the large number of tech transfer agreements with our allies]

System technology leaks where a lot of graduate students go back and forth. Technology is really an international language. The physical and scientific laws of nature have no barriers with ethnic groups or anything. It's been around since day one. People know the payoff.

I think there are two things though, a bottom line that you should keep in mind. You ask if we can control certain critical technology. Well, I think we have to realize that controls are short-lived at best. People are very bright and they're very intelligent and they're going to reverse-engineer it.

But, I think nonetheless as a nation we've done a very poor job. We can be smarter than other people, do different things to help protect our technology. I will mention in a generic way a case where we can be smarter. Let's take the CAT scanner in a hospital and say why we were concerned about it. Well, it was an embedded computing system with an ATP, GP and display, and a lot of software that could have been used off line for uses in which we didn't want it to be used. Getting together with the chief designer and so forth after four or five chats, there are ways that we can put engineering in there to prevent easy accessibility off-line or for reverse engineering.

Grant Dove, Senior Vice President, Texas Instruments Inc.

The critical argument in the Bucy report was the need to separate design and manufacturing know-how from end products and science. We believe this critical technology approach remains valid today as the only way to simultaneously achieve two goals: protecting the national security content of international trade and minimizing unnecessary restrictions of trade. Current efforts by the U.S. government to tighten controls over technology come against a heightened awareness of Soviet and other adversary nations' success in acquiring Western technology for use in the military efforts.

Denying or delaying Soviet acquisition of critical technology is, we believe, an accepted goal of the university commmunity, industry, and Government. Differences among Government, industry, and universities today occur over issues of definition and implementation.

The critical technology concepts should be distinguished from the militarily critical technology list [MCTL]. The critical technology approach was intended to identify the most important technologies and most active transfer mechanisms and focus control efforts on these. The militarily critical technology list is so long and the categories so broad that it does not appear to have the focus as was intended in 1976. The MCTL efforts should, therefore, not be regarded as fulfilling the concepts of the 1976 DSB report. The critical technology approach should not be submerged in short-term political consideration, such as economic warfare.

The critical technologies should not change during periods of détente and Cold War but provide the baseline of control areas both in the U.S. and with our CoCom allies.

The issue of controlling university research, which has created a lot of heat in recent months, goes much deeper than changes in Government regulations. Basic research in universities is not an issue. It should remain uncontrolled. The problem is that the old model of Government-funded basic research in universities that progresses toward applied research and eventually to military and later commercial applications simply does not apply today. Many universities are trying to build application labs in significant dual-use technology such a microelectronics. Since commercial applications for many of these technologies are preceding military use by several years, the results of these application labs should be covered by U.S. government regulations, just as they have been for years in industry.

But we must not forget that the economic vitality of our high-technology industrial base is of crucial importance to our nation's security. Since the Communist country markets are very small for most sectors, the primary impact of export regulations falls on free world trade. In designing a control structure, we must not "throw out the baby with the bath water." The critical technology approach could, in fact, facilitate East-West trade by placing less emphasis on controlling the end product.

And finally, we need to keep in mind the purpose of export control is to preserve technological lead time. Export control can delay the acquisition of critical technology by adversary nations but there's another side of the coin. That is the need for the U.S. to "run faster" in our own technology development and utilization in military systems.

After about 10 years of looking at it, we at TI are more convinced than ever that the critical technology approach has to be intelligently implemented no matter how difficult the test. It is essential that universities, industry, and Government go beyond rhetoric and ideology and seek pragmatic, workable solutions.

Robert Schmidt, Vice Chairman, Control Data Corp.

I have assumed that we have been convened here today with two objectives. First, to discuss the current and potential effects of the Government's policies for management of technical information on U.S. economic well-being. And, second, to make recommendations regarding current and future policies intended to manage the flow of technical operations.

In regard to the first objective, I want to make only one point, but I want to make it as strongly and as directly as I can. The point is that in my view the U.S. government is enmeshed in a myopic, self-deluding export-control process which has already cost the country billions of dollars in lost revenue and threatens to cost even more in revenues as well as in prestige, leadership, and security.

I call the process myopic because by focusing on restricting access to existing technology the Government is losing sight of the need to develop new technology. The 1979 version of the Export Administration Regulations seeks to control broad technologies and management skills as well as specific products. Its influence also extends to meetings, training agreements, technical exchanges, and workshops. The dilemma was summed up very nicely by five university presidents who wrote last year to the secretaries of commerce, state, and defense. In that letter they said restricting the free flow of information among scientists and engineers would alter fundamentally the system that produced the scientific and technological lead that the Government is now trying to protect and leave us with nothing to protect in the very near future.

The way to protect that lead is to make sure that the country's best talent is encouraged to work in the relevant areas, not to try to build a wall around past discoveries.

The other half of my opening assertion is that the export-control process is self-deluding. The reason for that statement is bound up with our arms-export policies and with the military critical list. As you know, the MCTL defines technology whose export is restricted.

[Quotes Rand report]: "But the most important question about technology transfer in the long run is whether the receiving side is able to absorb the technology it imports and to build upon it to generate further technological advances. In certain high-priority areas, notably military, where Soviet technological skills are already high, the Soviets' ability to learn from foreign technology is also high. But, in the industrial sector where most Soviet imports of foreign technology are concentrated the Soviets' record in absorbing and learning from it is poor." The Rand report concluded the most effective barriers against technology transfer are those directed by the Soviets against themselves. The Soviet difficulty in absorbing technology was not newly disclosed in the Rand report. It is a problem that was generally known for years. Yet, in response to this knowledge, the U.S. government persists in efforts to expand the MCTL, which already includes several hundred technologies, while aggressively maintaining its position as the world's No. 1 supplier of weapons to other nations.

President Reagan has eliminated nearly all the restraints on U.S. weapons exports. According to the *Defense Monitor*, over the past decade the United States has provided weapons and military services totalling more than $123 billion to about 130 of the world's 161 nations. This total includes 28 of the 41 militarily dominated governments. With this much of our own sophisticated weaponry in circulation, does the Government really believe that the embodied technology is safe from Soviet hands?

Iran is a recent example of the danger of providing sophisticated weapons to an unstable nation. With the fall of the Shah, the U.S. was in a position of having armed an adversary and having compromised secret military technology, particularly the F-14 and the Phoenix missile.

Not only have we made the technology generally available but we have even been thoughtful enough to provide it in the form in which it is most readily absorbed by the Soviets. Under these circumstances, the MCTL is an exercise in futility. In an analysis that my company has made of the list only 125 of its 700 technologies were found to be possible candidates for restrictive exporting and in many cases the restriction would have protected a proprietary process of particular companies rather than a technology that had any military significance. But given the extent of our arms traffic, the protection of any number of critical technologies is in question. The prime result of the MCTL is a loss of business by U.S. companies seeking to engage in free trade.

This brings me to the second objective for today which is to make recommendations for management of the flow of technical information. Ideally, the Government should bring its weapons-export policy into line with its position on other exports. Then in an effort to protect our truly advanced technology the MCTL should be revised and it should be shortened instead of broadened. The mistake being made is that the level of included technology is too low and that we are constructing a fence around past glories. An alternative approach would be to define as critical only technologies in which the United States has a clear lead. Those technologies would then become a part of the restricted export list. Two years might be used as a guideline for the list, and in those two years while other countries catch up to us we could realistically expect to advance further maintaining our lead. We would thereby protect only that which deserves protection, restore focus on leadership rather than on the status quo, and unleash our businesses to reestablish themselves in the world market. Achieving this will require hard work from all of us but I hope you will all agree that it is a far more rational and realistic approach than the witch-hunts that we are currently undertaking.

If we proceed in the fashion that we're now going and we don't take some advice from Fred [Bucy] in Texas Instruments, then we are soon going to be in the position where the only way to control what we need to control is to stop exporting. That's what I hear when I listen to all this discussion. It means stop exporting if we're going to get the kind of control that everybody thinks we ought to have.

William Howard, Vice President, Motorola Inc.

I think there are a number of points that I feel require some emphasis. The goal as originally stated for this technology control policy was to protect against a clear and present danger from the Soviet threat. And clearly we would agree that is a significant problem. There's another aspect of this that I think we have to be cognizant of and that is that although the Soviets represent a clear and present danger right now, there's also a clear and present danger which deals with the competitiveness of U.S. industry in worldwide markets. Speaking from my own industry, which is that related to the semiconductor industry, approximately 50 percent of the semiconductor market lies outside the United States. In fact, in many of the higher-technology areas, the United States does not have the monopoly on this technology. That's the important thing to remember.

In the discussions that took place earlier this year with respect to some of the items that were incldued earlier in CoCom discussions, one of the things that came up was the possibility of the potential controls on hyperpure silicon. It seemed to be new news to people who are proposing that silicon be controlled that, in fact, the majority of the hyperpure silicon made in the world is not made in the United States, and therefore a unilateral United States embargo in this commodity would in fact hurt only the United States and not cause substantial damage to the adversary.

The controls that have been put in place concentrate on means of transmission. Controls of commodities are very heavily dependent on shipping paperwork and on means of transmission. When we deal with information, we're dealing with something which is not a commodity type item but something which, once lost, can be replicated virtually indefinitely, and so controls on means of transmission are not the effective way to control this technology [information].

We have to look at the sources of information, not the means of transmission. There must be a cooperative agreement between the controlling authorities that are governmental, and those developing that information that are largely industrial, many of whom are not funded by the Government. In fact, the cooperative relationship must be symbiotic and must be equivalent for both sides, not just for one side or the other.

In the semiconductor industry there is a relatively limited number of sources of this kind of information which, if cooperative, could effectively bottle up a large part of this. But it has to be done in a way that the competitiveness of this industry does not suffer.

Classification as a means of controlling information is a major problem in that a lot of us in the civilian semiconductor industry don't have in place the facilities or the people to handle large amounts of classified activity. In fact, putting classifications as a control into this industry would be a major problem in the ability of technology to go forward. Instead we would prefer to rely

on items like employment agreements and other voluntary agreements by people working in this area as a means of controlling the flow of information.

The technology we develop is very definitely dual-use. As we pointed out earlier, applications of the civilian marketplace of critical technology frequently lead the applications in the military area. As a result, these [technologies] have to be viewed from the standpoint more of the Export Administration Regulation than from the standpoint of ITAR.

I believe that U.S. industry is willing to cooperate. Motorola has been involved in a lot of the activity that's going on in regard to militarily critical technology lists with regard to preparation of positions for CoCom, and we believe that industry is willing to cooperate in this activity because it's being recognized as a clear and present danger.

Furthermore, industry as a whole would welcome a slowdown in the inter-company as opposed to intracompany transfer of information as long as we are all provided with the same guidance. If we run into situations where foreign competitors show up with different sets of rules and conditions, then it represents a serious competitive threat to United States industry.

And finally a word of exasperation: Part 376 of the Export Administration Regulations in a world of highly-obfuscated governmental rules and regulations ranks as one of the most impenetrable documents that we have encountered. That is the section which deals with technical data transfer. Anything that can be done within the Commerce Department to simplify those regulations, or to clarify them would be a great benefit. Because we believe the majority of people in universities in the industry have no idea of what they mean and how to apply them.

Denysyk
A lot of people in government have the same feeling.

Erich Bloch, Vice President, IBM Corp.
I would like to focus on relationships internal to a company. We are a multinational company, and most of the high-technology companies are multinational companies that depend on the free relationship with their subsidiaries and with installations in foreign countries. Any amount of interference with that free relationship I think would be disastrous, not just for a company, but for the economy of the United States as a whole. I think we are not giving that kind of an aspect enough consideration. That means employment of foreign nationals, means information that has to flow freely on a daily basis—on an hourly basis, I would say—information sensitive to the company itself, that has to flow freely back and forth between these installations and the United States.

And by the way, let me make one point: the Government doesn't have a monopoly on how to protect information. I think the industry has learned the hard way and it has learned a great deal that it must protect its own information. I would urge that the Government use, as a part of its enforcement policy, the fact that the industry has an interest and an obligation to itself to protect its information in a serious kind of way. That should be a guarantee to the Government that information doesn't just free-flow all the way from here to everywhere it wants to go, but that information free-flows in channels that are controlled and required for the operation of the company. I want to really focus on that aspect of it: not just data flow to foreign countries, but data flow within the company itself. We should be careful that in our effort to restrict data flow and protect technology we do not restrict and inhibit the information, data flow, and technology transfer needed for the day-to-day operation of U.S. companies.

Denysyk
From some of the comments that you made earlier on where the problem is and how to solve the problem of technology transfer, it seems that we're looking at the problem as an either/or type of thing. We've focused simply on trying to control technology and not put enough emphasis on keeping our country ahead.

Frankly, I would agree with that. I don't think we have done enough to have an environment that's sufficiently fertile to encourage technology to progress and very quickly get into the different

factories so that we increase productivity. But it's not a one-sided issue. I think we need to look at both sides.

I think there is consensus in Government and perhaps in most other places that sombody has taken advantage of us. [The Soviets] have mechanisms to take technology that sometimes we view as purely civilian and put it into weapons or into logistical support very quickly. They have weapons coming on line every six or seven years.

Conversely, our weapons systems have large gaps in development, sometimes 10 or 15 years, but the Soviets always have a new system in the pipeline.

Just one other point—I don't think anyone in Government is trying to over-control the system. We took decisions in the past which were shortsighted in terms of economic and perhaps political strategic objectives. We have had problems in the past and the pendulum has swung too far in one direction.

But there is also a strong desire to construct a system which doesn't overcontrol so that the pendulum doesn't swing in the opposite direction and enter the domain where we start impeding legitimate technology transfers abroad, which would create markets where we can bring R&D dollars back into the United States to keep our technology going.

There's a very real desire on the part of all officials in Government to do that and we need advice as to how we can most effectively and most rationally construct a system like that.

One way of doing this is to look at the way the Bucy report suggests that we construct our control system. But even there it's not going to be a black and white situation. It's not going to be simply controlling technology and keystone equipment and decontrolling products. There are certain products which have their own intrinsic strategic value—large computers, for example, ATE, spectrum analyzers, and so forth.

So it will be an amalgam of various critical things: products, technology, and keystone equipment. But I think we're doing the right things. It'll take a little time, but I think we are going in the right direction. We welcome any kind of input that we can get from industry or from the scientific community to help us construct a rational system.

McMahon
Our study on technology transfers concluded not only that our technology was going into the Soviet weapons systems and causing us to spend more on our own defense, but that U.S. industry was being robbed. Your companies aren't getting a dime because the Soviets are stealing you blind, they're getting it for nothing through their intelligence services and that's why I say it's a counterintelligence problem, and industry is going to have to help figure out how to prevent it.

So it isn't a question of just trade, it's a question of U.S. industry being robbed.

Schmidt
If you can't export, you can't get money for it. That's the problem. Government is preventing industry from getting money for that technology, and I'll give you a classic example my friend, Gus Weiss [NSC staff], was involved in. We tried to export some obsolete memory disk products. We tried to export the ability for the Soviets to manufacture those disks without the technology for the head and we got turned down flat. My friend here said don't you do that, don't you even think about making a proposal. And that's about six years ago, as I recall, or longer. But anyway, next week at the National Computer Conference in Houston, Control Data is going to announce seven new products that cover the entire range of disks and not one bit of it has anything to do with the present technology. It's all plated heads and plated disks. It's a whole new technology. We could have in the process sold that other technology to the Soviets and got them started—they never throw anything away—gotten some money from it, and gone about our business, and they would be using that yet today.

McMahon
Well, I ask you to worry about the Soviets getting that plated technology today.

Schmidt
Sure, and they're going to try but we've got no more interest in letting them have that plated technology than you do and that's the point of my discussion. Let's get down to what's important and stop all of this horsing around with acetysalicylic acid [aspirin] which is one of the 700 things on the list. That's ridiculous; that denies the credibility of that list.

McMahon
I think to worry about trade and export is one thing; you also have to worry about them picking your pockets.

Schmidt
I agree with that; I don't question that for one second.

Henry Bachman, Vice President, Hazeltine Corp.
Someone made a comment that we had been taken advantage of and that's nothing new in the United States to be taken advantage of. We've got to be careful not to shoot ourselves in the foot in trying to prevent that from happening. There is some jeopardy in maintaining a free and open society, but we can't tie ourselves up in knots trying to prevent being taken advantage of.

Some of the additional regulations that we hear about today make you even more concerned when you hear the litany of things that we have to face in regard to doing our business, clearly not in the best interests of the country. Nobody here is arguing against the fact that the best thing for us to do is to stay ahead in our technology and the worst thing we could do is put obstacles in the way. But if we don't sell our products and make profits and justify investing money in R&D, we're not going to have that technology.

Industry recognizes very well the fact that it must protect from its competitors, be they domestic or foreign, those things that are important for its economic well-being. They should be relied upon more to do that voluntarily, rather than by imposing governmental regulations.

Edward David, President, Exxon Research and Engineering
I don't think the problems have been carefully defined. I don't think we really understand what we're trying to prevent. It's a very diffuse situation and I don't think the Federal agency people have done service to the community bringing the problem in this form. It would be much better if we understood clearly what is at issue.

But let's assume for the moment we do understand what the issues are. If you look at ITAR, CoCom, EAR, and the other mechanisms which we have used to try to regulate the flow of technology over the years, you have to say if there really is a serious problem today, these things haven't worked very well. Yet we hear proposals to augment mechanisms which apparently don't work.

This is a rather strange way of going about things. No matter how the regulations are changed, how the list is changed, whether we get new people in to operate the system, whether we have a more rational system in some sense, I don't think it's going to work a great deal better. I'm not being a defeatist. What I'm saying is that if you really want to control these matters, it must be done through a voluntary system in which the private sector plays an important role.

It's only by putting the responsibility where the critical information is that we will be able to get this problem worked out and indeed even get the problems defined. I don't believe you can define them on the general level that we've heard this morning. You have to consider industry by industry and probably company by company, and the only way to do that is to do it with the help of the private sector.

Now, I think we ought to spend some time this morning talking about mechanisms which would enable a good communcation between the private sector entities that have to be involved and the Federal entities that have to be involved and find some way of bringing these people together. I think that some of the things that have been said here this morning are certainly true. Industry is a responsible sector of society. Certainly the Government is a responsible sector of society. And if you want to define these problems and get solutions to them I think you've got to bring the responsible sectors together

Schmidt
I just want to say that I don't think there's ever been any disagreement between Fred Bucy and Bob Schmidt or even Lou Branscomb. We carried on a debate somewhat like this for the National Security Council at the beginning of the Carter administration. In fact, we've gone through this debate for about 12 years. It started in the Nixon administration. [**Ed David**—It goes back further than that.] One of the things that always happened was that each administration starts out like the world just began on January 20th. In this kind of situation, we have to have a policy that'll weather different administrations. And we're not getting it because our Government speaks with different tongues. Each department speaks with a tongue different from the other departments, and the Defense Department has two of them: the technical side, with Dick DeLauer's sort of position, and the strategic side with Fred Iklé. I'd just like to see us get one position in the Government that we can deal with, and then deal in a cooperative fashion. We've always said, "We've got to get on the same side of the table." We're not now. [**Henry Bachman**—Perhaps one could have something like the American Standards Association, something of that sort where one could set up standards and you could adopt them . . .]

Michael Lorenzo
I agree with Bob Schmidt and also with Ed David. We have four major things under way: Mapag renewing the MCTL, trying to get this down to a manageable size in terms of having it accepted; the Dale Corson National Science Foundation study; Dr. DeLauer and Dr. Kennedy of Stanford on the universities thing; and a meeting going on with Dr. Curry, vice president, Missiles Division at Hughes, heading up a Defense Science Board task force on technology transfer. Their first session is tomorrow, and they've been working quite a while. So—I hear you. But it ain't gonna happen overnight. What I've found in government—I've already been in several months—is this industry-government adversarial relationship. It's damn deep and heavy. I don't know how the hell you get rid of it. I've talked to a lot of old bureaucrats; I don't think they know they have it; they've never been in the private sector, they've never worked for a real profit, met a payroll, and I think you need more rotation of the bureaucrats in government and private sector and let them make a payroll, make a deadline, make a design, cut a piece of hardware, and produce it.

Jan Herring, Chief, Technology Transfer Assessment Center, CIA
I want to pick up on something that Ed David said, and that was about whether the old systems had worked. I think you've got to look at the environment in which they were forged. You didn't have the economic competition you do today. Nor did you have the intelligence threat that you have today, so I think you've got to look hard in planning a new system that handles all of these problems. We think that the old system has worked to some extent. It's forced the Soviet's and East European services to go to a very well-organized illegal program. They've acquired hundreds of millions of dollars of microelectronics production and design equipment illegally, and that doesn't go out of this country in a diplomatic pouch.

But it has gone out. It's been carted out of here, it's been taken from your subsidiaries abroad. If they need it, they will acquire it. You're not dealing with amateurs. The programs that they mount against you both for illegal trade and penetration of your company are well designed. Industrial security, the man from IBM said, is probably one of the best approaches that can be taken at the local level. And I think there's much to be said about that. But it's not the kind of industrial security we know today. It's not key-based defenses at the doors. Penetration of the Hughes Aircraft Co. is a good example of that; it's the recruitment of the man behind the door. This complicates your problem in trying to provide that kind of protection at the source. One other thing: when you look at the stealing, or the picking of your pocket, oftentimes the technology doesn't come back in the form of market competition. It doesn't show up outside the Bloc. But it does show up in the military arena. It forms a military threat to us and our allies. And that's very hard sometimes for people outside the intelligence commmunity to see because you don't have the classified materials to see that.

There are three trends we have seen over the '70s that will impact very heavily on the industrial security programs of the 1980s. First, the Soviet intelligence and East European intelligence services have been using these national intelligence means to acquire what we traditionally thought of as civilian technology: automotive technology, chemicals, energy microelectronics, and the consumer area. The second trend has been the emphasis on the part of Soviet and East European intelligence to acquire what we would consider to be the industrial, the production technologies, as opposed to the weapons technology. That's not unexpected because in many cases they're into the third and the fourth weapons generation. They don't need our weapons designs, but they do need a better productive capability to be able to manufacture the large volume needed by the Warsaw Pact. The third trend that we've noted is the focusing of Soviet and East European intelligence on the sources of our emerging technology: the universities, the commercial laboratories, at the point before it's protected. All three of those trends result in something that differs from the experience of the '50s and '60s—namely, the heavy emphasis of the Soviets and East Europeans on our commercial sector as opposed to our national security sector and the military labs where they design this work. It's oftentimes in that sector that the protection against Soviet intelligence, the counterintelligence, does not exist. Many of the Western countries do not provide counterintelligence protection for their commercial sector; companies really don't have the ability to counter this penetration effort on the part of the Soviets and East Europeans. And finally, that advanced commercial technology is in fact the technology that we're hoping to use in our military programs some years downstream.

Keyworth

Having sat here and listened so far, what I would like to do is make sure that I am extracting what I think is the general concensus.

Let me start with an extreme end on one side, which is the question of academic freedom. There's no question within the Administration that our academic freedom must be sustained, there's no question that it's one of the things that we have that serves us most effectively. However, the issue was raised that there is something new in terms of academic research. We think of academic research as being fundamental forefront-of-knowledge–type research. But what we are now beginning to have in some academic institutions is technology development, something very different from fundamental research. I would contend that at the present moment at least these are few and relatively far between and represent a very small part of academic research. VHSIC research is one example of an area of very serious potential leakage that is important, but I think it is dangerous if we allow that relatively local concern to, in any global way, strangle academic freedom. I think that Bobby Inman did this entire country a service regardless of the flack that he took for it by raising the warning at the AAAS six or eight months ago, the question and the concern. The discussion that has ensued has been a very productive and a very profitable one. But let me lay on the side academic research as generally a relatively small problem.

That takes me to a most informative discussion with Jan Herring some months ago . . . the CIA has been able to put together and bring out very, very clearly the fact that most Soviet military development has come straight from the United States. It is a very serious problem. But inevitably there will be technology transfer. The U.S. and Western world will inevitably help the Soviet Union do their development. And I think we have to accept that inevitability. The single most important issue that has come up today is the question of protecting existing technology versus tomorrow's technology. And it addresses the entire question of how we establish priorities. We have this global list of things we wish to protect—40 000 and more items depending upon which list you are looking at. We are trying to protect those, and granted the people who are actually doing the rule enforcement and regulation making are trying to use judgment to the best of their ability. But there is no built-in priority per se.

I can define two military technologies today that are absolutely critical for the future security of America. One is stealth technology and the other is antisubmarine warfare. They're both very, very forefront technology where we have a substantial lead over the Soviet Union and that must

be maintained. There are clearcut technologies that underlie that leadership and they are not as broad as saying all of microelectronics, either. But those should be examined by the Government to try to get industry involved in national security in detail so that very key elements can be identified and we can try to more rigidly draw fences around narrow things.

The Soviet Union's ability to penetrate has been very well testified to. Now, how are we in our free society, how will we control that? True we can't draw a fence around the country, but maybe we can draw a fence around very small local areas and thereby maintain our leadership. The counterexample I would offer is a personal example that I have run into before—we have protected the transfer of oscilloscopes, for example, to other nations for fear that they will use them in underground nuclear testing programs and extracting information. That's about a fourth-order payoff compared to what I was just defining as a first-order payoff. At least we ought to be able to distinguish the first from the fourth order.

First of all ,the lack of priorities is impeding industrial effectiveness. Secondly, it is probably making the job 10 times more difficult for the Government, and of course impeding the effectiveness of this overall control. The question has come up of an industrial-Government mechanism for starting with the problems of implementation and how fast it can be accomplished. It would seem to me that particularly the DOD hasn't a clearcut standing mechanism giving these priority assignments in areas that must be protected today, and lots more too than classified. The Department of Defense should have a standing or "a" mechanism, I won't even be as specific as that, a mechanism whereby you can have the kind of input-getting today getting down to brass tacks on specific issues and see how the implementation can best be perfected.

Schmidt
Your point, Jay, about that priority is critical to the whole damned discussion. I was trying in a maybe somewhat different way to make that very point. If we go back and think about the suggestion that was made by Fred Bucy's Defense Science Board report, I was always negative about that for a different reason. Not that I thought we shouldn't protect the technology but I was afraid that if the camel got its nose under that tent that we'd not only restrict the technology but we wouldn't release the product. And that's exactly what's happened. We have taken a very fine report and one with a lot of credence and bastardized it. And we've been at it since 1976. Now that shows you we weren't doing something properly.

Bachman
The last comment is one that I would've made. . . . We now have two kinds of restrictions; we have regulations on key technology and on products, and if we think of another mechanism we will have three sets of constraints unless we can do something to cut through all of this. The problem is that specific regulations come from the interpretation of more general legislative action. The only way you can get to that issue is you've got to start at the top, with the initial legislation.

Keyworth
There is no broad top-level Administration policy that has fully evolved on this subject. Cases keep coming up, often to the very top levels of the White House. For example, I recently attended a meeting where some key members of Congress wanted to talk to Ed Meese about this fifth-generation computer problem. There is an increasing level of awareness of this particular problem and there are groups working on it. But a broad policy stance is not yet evolved. At the beginning I said that I thought that industrial competitiveness and what we are trying for the U.S. to constrain from the Soviet Union are two very different things but they overlap. The United States and most of the rest of the Western world are just plain very, very different countries. The reason, of course, is that whether we like it or not, we still retain fundamental responsibility for security in the West. It is our military technology that really underlies that superiority. That places a very different responsibility on the United States.

So how do we come into the new era of competitiveness and still address this problem of

technology transfer? Today does require new solutions. I think most people agree that we are not going to maintain either our fundamental scientific or even our sorely challenged technological superiority unless we find new solutions to today's problems, and I think one of the best things we have come up with today really is a number of comments that say the assumptions behind this question of transfer to the Soviet Union for the last 20 years are no longer the same.

Schmidt
In these discussions and some others I've been in frequently we intermix the question of military security and strategy with the question of national security and strategy and the two are not always the same. And they must be handled and treated in different ways. If we had a good, sound military strategy, which I don't really think we have, we could sovle a lot of those arguments and questions about what's good and what's bad to export. And if we also had a good, sound national security strategy we could then unmix the two and we wouldn't get all confused.

Donald Langenberg, Deputy Director, National Science Foundation
I want to solicit views around the table on a different aspect of this question than we've discussed so far. By far the most effective means of technology transfer is the head and the hands of a human being. And one of the biggest import/export businesses this country has had in the last three decades is higher education. We have "processed" through our institutions of higher education hundreds of thousands of foreign nationals. They tend to concentrate in our schools of engineering and science departments.

Some stay and they pass from being foreign nationals to immigrant aliens to citizens and wind up playing key roles in American high technology. Some return home and achieve positions of leadership, technical or political leadership, in their own countries. And they do so for better or for worse as alumni not only of our institutions of higher education but of the United States. I'd like to hear the views of any of you on the Government or industrial side about how we deal with these people.

Keyworth
I think that the export, as you call it, of students and of expertise, knowledge, and so on is one of the proudest that this country has. I believe that the openness of our academic institutions to foreign students should be maintained, even increased, that we should be proud of the fact that 50 percent of our graduate students in engineering are from other nations. I think that this is a testimony to our society and it is one of the unattractive aspects of isolationism that many people have questioned whether this is in America's best interest to have so many foreign students.

Bloch
I agree with what you're saying. There are clearly lofty reasons for keeping it open, and selfish reasons also. Where would U.S. industry high technology be today if it were not for foreign immigrants, for people that are here for a long period of time? Secondly, even if they go back, how many of these people are being hired by and are therefore supporting, directly or indirectly, American companies operating overseas?

Gordon Moore, Chairman, Intel Corp.
I agree with a good portion of this. Aliens certainly have been a major source of personnel for a company like ours. But don't underestimate the loss of information that can occur this way in a very new technology. By the time you get the body of information that exists in microelectronics today, for example, probably no two people could transfer a significant portion of it.

But in one of our newer areas, in microelectronics 10 years ago, for example, one graduate student properly positioned can take back a tremendous amount of information. Seeing Polish graduate students at Stanford at that time really bothered me. This is a potentially major leak of information, and I think you do have to be careful if you're really concerned about the loss of information [illegible]

Denysyk
Back to what Jay said earlier, about the need to keep a fairly open scientific environment in universities: I don't think anyone in Government is trying to control that, even for Bloc countries.

Our concerns do not lie in open-literature basic research and present controls are not directed at foreign students in the aggregate. They're directed to a very narrow sector of technology: technology in the sense of process know-how, not the basic research, not the systematic exploration of new frontiers, but rather the application of that knowledge into industrial processes, how to make things, how to make chips.

Cornell University comes to mind immediately in terms of applications laboratories, and Stanford for robotics. Those types of research have fairly direct and significant applications in the military infrastructure, to make weapons to increase produce. In terms of people, though we're interested in depriving nationals from proscribed countries of easy access to this technology, it's clear that we can't hold a wall high enough to prevent all leaks of our technology.

Nor would we want to because [censorship] will spill over into other areas and we'd lose creativity. The people we want to keep that technology from are the Communist country nationals, Eastern Europe, USSR as well as PRC. So if you extract those sectors out of the whole aggregate of academia, they are minimal. I think you can construct a reasonably rational system to minimize this danger without impacting on scientific creativity. I think it is a fairly small and reasonably well-defined problem, and if we attack it as such I think it's manageable.

Rubinstein
Does it seem there ought to be some sort of an ongoing industry-Government effort? Certainly *Spectrum* doesn't want to be in the business, but would it be in the interest of this group for us just to try to offer our services to find the people that might organize such a thing and just sort of start it going and step out of it?

Gus Weiss, Staff Member, National Security Council
The world doesn't need another group. As Steve Bryen pointed out earlier, we're all tied up, being awfully low on staff. The people who work this problem are finite in number and have got weighty responsibilities, so unless you can come up with a clear definition of what that would do and how that would help, I'd be skeptical about tying up expensive people's time.

We haven't mentioned an opportunity coming up which you might want to think about as an alternative, namely the rewriting of the Export Administration Act, which comes up next year for renewal. Many of the things that had been mandated and methods by which we're operating are in the present act. I'm sure that that would be a weighty and very controversial and important effort for everybody concerned in industry, Government, and the Hill—to find out what provisions need to be changed and whether the list needs to be continued and so on, can do some yeomanlike work by putting together whatever it is you're capable of doing to comment on that. That's the thing we're looking forward to as sort of the next thing. I would point out that those of us who struggle with this—and I think I'm the last person in the Government who was on the Bucy panel—are convinced that this is about the most elusive subject you could get at. If you listen to the shades of color going around the room, we have a counterintelligence problem, a university problem, a basic research problem, an applied research problem, different technologies, 27 different Government agencies up against a very professional collection service cutting off exports for some allegedly myopic reasons, and a lack of priorities.

In fact, it's not that we don't have the priorities straight, it is that they conflict with each other, and the only time that we ever really sat down and did a methodical review of the conflicting priorities, namely economic strength versus technological loss, was a study of computer sales to Soviet countries done in 1974. There we quantified the whole thing as best we could in a crude way and that became a CoCom position.

Barring that one attempt, it's really a very hard thing to do as everybody knows. And antitrust is a minefield and I don't know who's got the minesweeper to go through and work that. Well, I'll just conclude by saying that I would hope we could begin to focus on the Export Administration Act and what can be done through that to help straighten this out. And if people want to come to see NSC, they are welcome to come by. I'd be happy to talk.

Keyworth
I find that I will confess to a significant lack of personal confidence, let's say, in how the bureaucratic mechanisms of the past are likely to be effective in the future in preventing what has built up to be an overwhelming problem. Certainly, it has worked in the past in the sense that it just forced the Soviet Union to become better but nevertheless the ability of the Soviet Union to target the flow of technology is vastly superior to what it was in the past.

I do think new mechanisms are needed here. Just another plain study group is not what I thought anybody was discussing. We were talking about a mechanism which I couched in terms of priorities to be established. Efforts should be made to develop a close-standing interaction between defense, in particular, and the private sector, and I for one still feel it would be a valuable thing, and I would be delighted to sit down and talk with Dick DeLauer about it and maybe John McMahon would also like to participate.

John Ellicott, Partner, Covington & Burling
I would just like to make a plea for simplicity and against overregulation. I completely concur with what Mr. Weiss has said about not having too many study groups but I'm not sure I agree with him on the Export Administration Act. In my view there's too much in it already, and the problem, if it exists, is one of more effective enforcement in some of these areas and perhaps a degree of better industry self-policing. I have a feeling industrial security is very good in some areas and perhaps not as good as it should be in other areas. I don't think that what we need is a great new regulatory scheme. We especially don't need something that's going to impose a mass of new rules to affect communications within companies or within the Western world. Although I agree with Dr. Keyworth that the United States has a special position of leadership when it comes to Free World security, we do not have a monopoly any more and we have to get cooperation from our friends in Western Europe. If we try to do it unilaterally through a large and extraterritorial type of control scheme it will not work.

Rubinstein
I was looking for a mechanism by which the time that you gentlemen spent coming here would yield something that might be of some continuing benefit. Since I had heard several people say that there ought to be more industry-Government, at least industry-DOD contact, I thought maybe since all of you are very busy, we could at least try to find a couple of people who would sit and think about it for a little bit and make a proposal back to you.

We will offer our services to try to outline a narrowly scoped follow-up and if anybody wants to suggest something to us, we would be happy to do it. And if it turns out that it's not in harmony with what any individuals here would like, we will find out very quickly I'm sure.

Unattributed statements

(Various meeting participants indicated that they would prefer not to have their names attached to certain statements. Since the material they wished to dissociate themselves from is nonetheless pertinent, it has been included here.)

As a result of Afghanistan we got agreements from the allies that they would cut back considerably the exceptions that they would request on shipments to the Soviet Union. And subsequently after the invasion of Poland, we approached them the same way.

The (CoCom technical subcommittee) endorsed the U.S. initiatives on the need to limit the access of Soviet businesses to control technology and on limiting Eastern access to Western data banks.

We have also seen reluctance on the part of other governments (in CoCom) to devote additional resources to enforcement efforts.

In the past, CoCom as an organization worked largely on the rule of exception, and so the actual rules become blurred. In a sense, CoCom could be understood as an organization that ratified export decisions that in themselves were not quite harmful.

References

(These references were supplied to round-table participants either prior to or at the meeting and furnished a background for discussion.)

1. "Soviet Acquisition of Western Technology," U.S. Central Intelligence Agency, April 1982.

2. "Selling the Russians the Rope? Soviet Technology Policy and U.S. Export Controls," Thane Gustafson, Rand Corp., April 1981. (R-2649-ARPA). Executive summary only.

3. "Controls on the International Transfer of Scientific Information," Richard Meserve, March 1982. A report to the National Academy of Sciences panel on scientific communication and national security.

4. "Technology and East-West Trade," Office of Technology Assessment, 1979. Executive summary only.

5. "An Analysis of Export Control of U.S. Technology—a DOD Perspective," Office of the Director of Defense Research and Engineering, Feb. 4, 1976 (The "Bucy Report"). Executive summary and conclusions only.

(Other references, as well as information on other initiatives in this area, may be found in the articles on information control in the May 1982 issue of Spectrum, *pp. 64-73, and in the September 1982 issue of* Spectrum, *p. 66-70.)*